

NASA Conference Publication 3356

L_f97 Fourth NASA Langley Formal Methods *fm* Workshop

Compiled by
C. Michael Holloway and Kelly J. Hayhurst
Langley Research Center • Hampton, Virginia

Proceedings of a workshop sponsored by
the National Aeronautics and Space Administration,
Washington, D.C., and held at the Radisson Hotel,
Hampton, Virginia
September 10-12, 1997

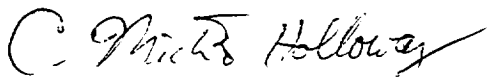
September 1997

General Chairman's Message

On behalf of the Langley Formal Methods Team, I welcome you to Lfm97, the Fourth NASA Langley Formal Methods Workshop. The primary purpose of our workshops has always been to bring together leading formal methods researchers and practicing engineers in an environment in which each group can learn from the other. The three previous workshops were limited to invited presentations, but we expanded this year's workshop to include 17 submitted papers. We believe that the program has something to offer to everyone, from those interested in the theoretical aspects of formal methods to those interested in the practical application of formal methods to help solve real problems. I hope that you will agree, and that you will find your time at Lfm97 both interesting and useful.

Many of the slide presentations that will be given at the workshop will be available on the World-Wide Web at <http://atb-www.larc.nasa.gov/Lfm97/>. Information on the NASA Langley formal methods program is also available on the web at <http://atb-www.larc.nasa.gov/fm.html>.

I look forward to meeting you during the workshop. Please let me know if there is anything that I can do to help you while you are here.



C. Michael Holloway, Lfm97 General Chairman

E-mail: c.m.holloway@larc.nasa.gov

Postal Address: Mail Stop 130, NASA Langley Research Center, Hampton VA 23681-0001



Workshop General Chairman

Michael Holloway, NASA Langley Research Center

Program Committee

Ricky Butler, NASA Langley Research Center (chairman)

Jim Caldwell, NASA Langley Research Center

Victor Carreño, NASA Langley Research Center

Ben DiVito, ViGYAN

David Guaspari, Odyssey Research Associates

Kelly Hayhurst, NASA Langley Research Center

Michael Holloway, NASA Langley Research Center (acting chairman)

Damir Jamsek, Odyssey Research Associates

Pat Lincoln, SRI International,

Paul Miner, NASA Langley Research Center

John Rushby, SRI International

Organizing Committee

Kelly Hayhurst, NASA Langley Research Center

Michael Holloway, NASA Langley Research Center

Lisa Peckham, NASA Langley Research Center

Pamela Verniel, NASA Langley Research Center

Sponsoring Organization

Assessment Technology Branch,
Flight Electronics Technology Division,
Research & Technology Group,
NASA Langley Research Center,
Hampton, Virginia, U.S.A.

Table of Contents

General Chairman's Message	iii
Lfm97 Organization	v
Why Are Formal Methods Not Used More Widely?	1 -1
<i>John Knight, Colleen DeJong, Matthew Gobble, and Luís Nakano</i>	
Plotting The Escape from The Tower: A Formalist's Practicality Primer	13 -2
<i>James Sutton</i>	
Proving Properties of Accidents	21 -3
<i>C. W. Johnson</i>	
Formalization and Analysis of the Separation Minima for Aircraft in the North Atlantic Region 35	4
<i>Nancy Day, Jeffrey Joyce, and Gerry Pelletier</i>	
Modeling and Validating SAFER in VDM-SL	51 5
<i>Sten Agerholm and Peter Gorm Larsen</i>	
Requirements Analysis of Real-Time Control Systems Using PVS	65 -6
<i>Bruno Dutertre and Victoria Stavridou</i>	
Reuse of a Formal Model for Requirements Validation	75 -7
<i>Robyn Lutz</i>	
Applying the SCR Requirements Method to a Simple Autopilot	87 -8
<i>Ramesh Bharadwaj and Constance Heitmeyer</i>	
A Tabular Language for System Design	103 -9
<i>Steven Johnson</i>	
Verifying Communication Related Safety Constraints in RSML Specifications	115 -10
<i>Mats P.E. Heimdahl</i>	
Towards High-Assurance High-Performance Program Synthesis	129 -11
<i>Michael Lowry, Steven Roach, and Jeffrey Van Baalen</i>	
On the Automatic Discovery of Loop Invariants	137 -12
<i>Andrew Ireland and Jamie Stark</i>	
PV: A Model-Checker for Verifying LTL-X Properties	153 -13
<i>Ratan Nalumasu and Ganesh Gopalakrishnan</i>	
Automated Deductive Verification of Parallel Systems	163 -14
<i>Hassen Saïdi</i>	
Robust Computer System Proofs in PVS	177 -15
<i>Matthew Wilding</i>	
Domain Checking Z Specifications	185 -16
<i>Mark Saaltink</i>	
Fundamental Hardware Design in PVS	193 -17
<i>James Leathrum, Jr.</i>	